

ADR

ORIGINAL

1 Michael W. Sobol (State Bar No. 194857)
 2 LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
 3 275 Battery Street, 30th Floor
 4 San Francisco, CA 94111-3339
 Telephone: (415) 956-1000
 Facsimile: (415) 956-1008
 msobol@lchb.com

5 *Attorneys for Plaintiff and the Proposed Class*

E-Filing FILED

DEC 22 2011
 RICHARD W. WIEKING
 CLERK, U.S. DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA

B
 # 99
 deep
 NP

6 UNITED STATES DISTRICT COURT
 7
 8 NORTHERN DISTRICT OF CALIFORNIA
 9
 10 (San Jose Division)

HRL

11 Michael Allan, on behalf of himself and all
 12 others similarly situated,

13 Plaintiffs,

14 v.

15 CARRIER IQ, INC., a Delaware
 16 corporation; HTC CORPORATION, a
 17 Taiwan corporation; HTC AMERICA,
 18 INC., a Washington corporation; and
 DOES 1-100,

19 Defendants.

Case No. CV 11-06613

CLASS ACTION COMPLAINT FOR
 VIOLATIONS OF 18 U.S.C. § 2511 AND
 THE CALIFORNIA UNFAIR
 COMPETITION LAW

DEMAND FOR JURY TRIAL

20
 21 Plaintiffs, by and through their attorneys, bring this action for damages and
 22 equitable relief, on behalf of themselves and all others similarly situated, against the above-named
 23 Defendants, demanding a trial by jury, and allege as follows:

24 PRELIMINARY STATEMENT

25 1. Unbeknownst to millions of American mobile device owners, Defendants Carrier
 26 IQ and HTC have designed and installed software called IQ Agent on millions of cell phones
 27 and other mobile devices across the country. IQ Agent records and transmits to cellular carriers,
 28 such as Sprint and AT&T, data relating to customers' cellular phone use. The data are then

FAXED

1 analyzed and segmented, including by equipment and subscriber identification numbers. IQ
 2 Agent cannot be removed and cannot be detected by users lacking advanced computing skills.
 3 Users are not notified of its presence, nor are they asked to agree to its operation.

4 2. Published research into IQ Agent's functioning reveals that the software records
 5 numerous types of information for transmission to its customers, including the path of web
 6 addresses meant to be transmitted securely via the HTTPS protocol between users and the web
 7 servers they visit. In this, Carrier IQ's software IQ Agent intercepts electronic communications
 8 that users intend to be "secure," *e.g.*, bank account numbers, user names, passwords, and search
 9 terms.

10 3. Because of its use and function, Carrier IQ's software transmits private
 11 telecommunications and electronic information in violation of federal wiretap laws, California
 12 computer abuse laws, and the common law of invasion of privacy.

13 **JURISDICTION AND VENUE**

14 4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331.

15 5. This Court has supplemental jurisdiction over Plaintiffs' state law claims
 16 pursuant to 28 U.S.C. § 1367(a).

17 6. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants
 18 reside, transact business, are found in, or the claims arise in part, in this District.

19 **INTRADISTRICT ASSIGNMENT**

20 7. Venue is proper within the San Jose division of this District under Local
 21 Rule 3-2(c) as a substantial part of the events or omissions which give rise to the claims herein
 22 occurred in San Jose.

23 **PARTIES**

24 8. Plaintiff Michael Allan resides in Liberty, Kentucky.

25 9. Defendant Carrier IQ, Inc. is a company with its principle place of business in
 26 Mountain View, California and offices in Boston, Chicago, London, United Kingdom, and
 27 Kuala Lumpur, Malaysia. Carrier IQ creates the software that is the subject of this Complaint.
 28

Carrier IQ sells its software IQ Agent to cellular carriers and creates customized software packages for mobile device manufacturers to install on their products.

10. Defendants HTC, Corp. and HTC America, Inc. are companies with their principle place of businesses in Bellevue, Washington. HTC Corp. is the parent company of HTC America ("HTC"). HTC designs and manufactures mobile devices known as smartphones, including Plaintiff Michael Allan's HTC EVO 4G, and sells them throughout the United States.

11. DOES 1-100 are third parties whose identities are presently unknown to Plaintiffs, but who are responsible in some manner for the violations herein alleged. Plaintiffs will amend this complaint to allege the names and capacities of these defendants when they have been ascertained.

FACTUAL ALLEGATIONS

I. Carrier IQ Sells Its Software "IQ Agent" To Cellular Carriers And Mobile Phone Manufacturers So They Can Track And Analyze Users' Experience.

12. Carrier IQ has been operating since 2005 as a provider of software for cellular carriers and mobile phone manufacturers.

13. Carrier IQ offers its customers, as its motto claims, "The Power of Knowing." Its software is now installed on over 140 million mobile devices worldwide.

14. Carrier IQ states on its Web site that it has grown to become the "market leader in Mobile Service Intelligence solutions that have revolutionized the way mobile operators and device vendors gather and manage information from end users."

15. Carrier IQ sells its "Mobile Service Intelligence" solutions to mobile phone manufacturers and cellular service providers. On its website, the company touts its "unique ability to provide detailed insight into service delivery and user experience." Carrier IQ promises its customers: "you can achieve your strategic goals more efficiently and effectively, based on data drawn directly from your subscribers' devices — the place where your customer actually experiences the service."

1 16. Carrier IQ's Mobile Service Intelligence solution relies on its "unique ability to
2 analyze in detail usage scenarios and fault conditions by type, location, application and network
3 performance."

4 17. Carrier IQ's central product is its Mobile Service Intelligence Platform (MSIP),
5 which "receives raw data (known as Metrics) from phones and converts them into reliable,
6 repeatable Measures which feed into analytic applications."

7 18. In particular, Carrier IQ's "Insight Experience Manager uses data directly from
8 the mobile phone itself to give a precise view of how users interact with both their phones and
9 the services delivered through them, even if the phone is not communicating with the network."

10 19. Carrier IQ promises that its Experience Manager will allow carriers or
11 manufacturers to "[i]dentify exactly how your customers interact with services and which ones
12 they use. See which content they consume, even offline." This includes allowing carriers and
13 manufacturers to "view application and device feature usage, such as camera, music, messaging,
14 browser and TV."

15 **II. Hidden And Inaccessible, Carrier IQ's Software "IQ Agent" Was Recently**
16 **Discovered, Causing A Public Outcry Over Its Impact On Consumer Privacy.**

17 20. In mid-November 2011, mobile developer Trevor Eckhart published a report on
18 his website detailing his discovery of a piece of software running on his HTC smartphone called
19 IQ Agent, which is designed by Carrier IQ. Eckhart raised questions regarding what function IQ
20 Agent serves and what information it has access to in its normal operation.

21 21. Eckhart discovered that IQ Agent is a hidden, irreplaceable, permanent piece of
22 software. Unlike all other applications and services on the Android mobile operating system, IQ
23 Agent cannot be identified, terminated, or removed without advanced computing and
24 development skills.

25 22. Based on his initial investigation, Eckhart concluded that Carrier IQ's IQ Agent
26 is a "rootkit," defined by Wikipedia as "software that enables continued privileged access to a
27 computer while actively hiding its presence from administrators by subverting standard
28 operating system functionality or other applications Although rootkits can serve a variety

1 of ends, they have gained notoriety primarily as malware, hiding applications that appropriate
2 computing resources or steal passwords without the knowledge of administrators and users of
3 affected systems.”

4 23. Following the initial report, Carrier IQ sent Eckhart a cease and desist letter
5 demanding that he retract his description of the software as a “rootkit.”

6 24. The Electronic Frontier Foundation (EFF), which advocates for the freedom of
7 speech and openness in the technology field, responded on behalf of Eckhart and Carrier IQ
8 quickly withdrew its demand. The conflict between Eckhart and Carrier IQ sparked public
9 interest. Eckhart himself decided to investigate the software further.

10 25. The result of Eckhart’s investigation was a seventeen minute video, posted on
11 YouTube and his website, illustrating in detail how IQ Agent interacts with his HTC
12 smartphone. The video can be found at http://www.youtube.com/watch?v=T17XQI_AYNo (last
13 accessed December 5, 2011).

14 26. The video details IQ Agent’s functioning within the Google Android mobile
15 operating system on Eckhart’s HTC smartphone. Eckhart concludes that IQ Agent functions
16 more or less identically on other manufacturers’ Android phones as well.

17 27. Eckhart’s video sparked extensive public interest in the previously unknown
18 software and the company that created it. Thousands of articles and blog posts have examined
19 Eckhart’s video and the potential impact of a piece of hidden software having access to users’
20 sensitive information.

21 28. For example, the technology website *Gizmodo* (gizmodo.com) has published
22 numerous articles relating to Carrier IQ and IQ Agent. Its initial article was headlined “Your
23 Android Phone is Secretly Recording Everything You Do,” accompanied by a graphic stating
24 “YOUR PHONE IS WATCHING YOU” and the picture of a phone with a hole through which
25 an unidentified man is watching the user.

26 29. Public interest in Carrier IQ has also led to an informal U.S. Senate inquiry from
27 Senator Al Franken, who sent Carrier IQ a letter expressing concern over its software’s impact
28 on consumer privacy and requesting more information.

30. Numerous websites have also published information on how Android users can check to see if IQ Agent is running on their phones.

III. IQ Agent Records Vital User Information And Transmits It To Cellular Carriers, Including Web Addresses That Are Meant To Be Secure And Encrypted Because They Contain Sensitive Information.

31. Following the initial public outcry over the discovery of IQ Agent, researcher Dan Rosenberg investigated the internal functioning of Carrier IQ's software.

32. Rosenberg uncovered a list of "metrics" that IQ Agent records without users' knowledge. These metrics are captured and then transmitted to Carrier IQ's customers — cellular carriers such as AT&T and Sprint, or to Carrier IQ's servers.

33. Rosenberg confirmed that IQ Agent operates in the background of Android devices at all times, situated between the user and the operating system. The software logs extensive amounts of information about users' experience, including but not limited to:

- when users turn their mobile devices on or off;
- which applications users download, open, and close;
- which applications crash on users' devices;
- where users' devices are located;
- whether calls or text messages are received by users;
- which websites users visit;
- whether the websites users visit load properly;
- whether users' screens are on or off;
- which keys users press on the phone dialer, even if the phone numbers are not dialed;
- user devices' battery level, voltage, and temperature;
- and most shockingly, users' passwords and other private information entered into websites, including encrypted websites with the HTTPS prefix.

34. The most concerning of Rosenberg's discoveries is that IQ Agent, because it functions as a rootkit, intercepts communication between the internet browser and the web server a user visits, even when the user visits a website secured by the HTTPS internet protocol.

1 35. The HTTPS protocol allows users to enter sensitive information such as
2 passwords into their internet browsers, and it sends it to the web servers they visit via an
3 encrypted method. It is represented by the "https://" prefix as opposed to the regular "http://"
4 prefix at the beginning of a web address. For example, Bank of America's secure online
5 banking portal can be accessed at https://www.bankofamerica.com. When users type
6 http://www.bankofamerica.com, they are automatically re-routed to the "https://" version of the
7 site.

8 36. This protocol is commonly used in transactions that involve sensitive information
9 such as credit card numbers, bank account numbers, and usernames and passwords. The HTTPS
10 protocol makes it impossible for external parties to intercept the traffic between users and the
11 websites they visit because it encrypts the data exchanged between them. Consequently, users
12 believe that they can shop online, bank online, and otherwise enter sensitive information online
13 without third-party interference or interception when using the HTTPS internet protocol.

14 37. For example, users who log into their e-trade.com brokerage accounts visit a web
15 page secured by HTTPS. The information that users enter into their e-trade.com account
16 remains private and can only be accessed by e-trade's servers.

17 38. On e-trade.com's web pages, the web address, or "URL" in the browser
18 sometimes reflects the e-trade.com user's brokerage account id, *e.g.*,
19 https://etws.etrade.com/accounts/rest/accountbalance/{AccountId}. In a normally-functioning
20 computer or Smartphone, this URL would not be accessible by third parties, and thus does not
21 pose a risk to the user of third-party interference or interception of their brokerage account id.
22 The portion of the URL that contains the account id would be encrypted and therefore
23 indecipherable by the outside world.

24 39. Despite the design of HTTPS, IQ Agent can intercept HTTPS URLs and record
25 them before they are encrypted. In the example above, IQ Agent would capture the entire URL,
26 including the brokerage account id, despite the widely-held and advertised notion that online
27 banking and trading is secure thanks to the HTTPS internet protocol. In this, IQ Agent functions
28

1 similarly to a host of third-party malware and nefarious software intended to steal passwords and
 2 other sensitive information. Some of these are known as “Man-in-the-Middle” attacks.

3 40. The HTTPS internet protocol is not only used by Smartphone browsers.
 4 Smartphone apps, such as apps available on the Android Marketplace, also may utilize HTTPS
 5 to send and receive secure information. In such a situation, Carrier IQ again captures the URL
 6 information despite its design as a secure protocol.

7 41. Thus, because of its design and its interception of HTTPS URLs, IQ Agent is
 8 systematically capturing and transmitting data to cellular carriers that is meant to be private and
 9 is widely known and advertised to be private and inaccessible by third parties.

10 42. Moreover, IQ Agent also records details on application usage. In particular, IQ
 11 Agent reports to cellular carriers which applications users download and how much they use
 12 them. This is particularly shocking considering the fact that many users choose Android devices
 13 instead of other devices because they have an un-regulated application marketplace — a
 14 marketplace that allows them to use applications that would otherwise be rejected for reason of
 15 gratuitousness or controversy.

16 **IV. Carrier IQ Affords Cellular Carriers The Ability To Analyze Users’ Information**
 17 **For Their Own Purposes, Including For Marketing Purposes.**

18 43. The information captured by Carrier IQ’s software IQ Agent is transmitted to
 19 cellular carriers either via storage on their web servers or on Carrier IQ’s. Carriers then use
 20 Carrier IQ’s proprietary web portal to access user information in a variety of ways.

21 44. For example, Carrier IQ’s “IQ Insight Experience Manager” promises customers:
 22 “IQ Insight enables you to align your business improvements with the things customers truly
 23 value. Identify exactly how your customers interact with services and which ones they use. See
 24 which content they consume, even offline.”

25 45. Carrier IQ’s “IQ Insight Experience Manager” provides its customers with
 26 “Actionable Intelligence” on their customers. For example, Carrier IQ claims their customers
 27 can use this intelligence to answer “business-critical questions, including: How long does it take
 28 the user to start the service?” and “How do users respond to mobile advertising?”

46. Carrier IQ specifically advertises to customers the ability to: "View application and device feature usage, such as camera, music, messaging, browser and TV."

47. In a press release issued June 8, 2011, Carrier IQ touted a recent marketing analysis it performed with its mobile intelligence tools: "'In a recent operator rollout of Carrier IQ's application analytics, we were able to demonstrate that if Facebook was preloaded on a specific Smartphone, 40% of the app usage from that device in the first month was with Facebook. Without the preload, it was only 5%, as users had to download the app themselves,'" said Andrew Coward, Vice President of Marketing at Carrier IQ."

V. HTC Installs IQ Agent on Its Android Devices At The Behest Of Cellular Carriers

48. Numerous cellular carriers, Android device manufacturers, and Carrier IQ have all confirmed that manufacturers alter the Android code in order to integrate IQ Agent at the behest of cellular carriers.

49. HTC has installed IQ Agent on Plaintiff's phone as well as millions of others at the behest of cellular carriers.

50. HTC has not sought or received the consent of its customers, including of Plaintiff, to install IQ Agent on their mobile phones.

VI. Carrier IQ and Cellular Carriers Claim That Carrier IQ Is Safe And Does Not Violate Consumer Privacy Interests.

51. Carrier IQ and its customers have responded forcefully to claims that IQ Agent has violated consumer expectations of privacy.

52. On its website, Carrier IQ claims that its technology encrypts and makes anonymous the user information that it records and sends to its customers.

53. In two public statements, Carrier IQ has claimed that its software does not record keystrokes, provide its customers with tracking tools, or report on the content of private messages. Instead, Carrier IQ claims that its software produces secure, anonymous, aggregate data for carriers and manufacturers to evaluate the performance of their hardware and networks.

54. Thus far, cellular carriers AT&T, Sprint, and T-Mobile, along with hardware manufacturers HTC and Samsung have confirmed that their phones integrate the Carrier IQ

1 software. Verizon Wireless, Research in Motion (the maker of the Blackberry smartphone),
 2 Microsoft, and Nokia have all strenuously denied claims that their phones use Carrier IQ. Apple
 3 has indicated that it formerly integrated Carrier IQ into its iPhone, but that it no longer uses the
 4 software.

5 55. HTC and Samsung have stated that they integrated IQ Agent into their hardware
 6 solely at the behest of cellular carriers.

7 56. All carriers and manufacturers who use IQ Agent have claimed that it is used
 8 solely for the purpose of improving network performance and user experience; the companies
 9 have variously indicated that they do not receive or seek private information that is not
 10 anonymous or unidentifiable.

11 **VII. Carrier IQ's Claims Regarding The Safety Of Its Software Are Inaccurate And**
 12 **Misleading.**

13 57. The results of Trevor Eckhart and Dan Rosenberg's investigations into IQ Agent
 14 undermine Carrier IQ's claims that its software is safe and does not violate consumer privacy.

15 58. In particular, Eckhart and Rosenberg demonstrate that IQ Agent does, in fact
 16 record various types of private information.

17 59. Eckhart's research also demonstrates that Carrier IQ utilizes its servers to record
 18 information about users and their mobile phones. Most importantly, Eckhart demonstrates that
 19 Carrier IQ's online portal for its customers identifies phones by their equipment and subscriber
 20 identification numbers, wholly undermining Carrier IQ's claim that its information is
 21 transmitted anonymously.

22 60. Carrier IQ and its customers have, in fact, confirmed that the information
 23 recorded on users' mobile phones is transmitted both to Carrier IQ and to its customers.

24 61. Carrier IQ has also confirmed that its products include a "customer care" solution
 25 that offers cellular carriers the ability to gather information about particular mobile devices and
 26 *identify the owners of those mobile devices* in order to provide them custom-tailored customer
 27 care. Carrier IQ give the example of carriers examining the applications downloaded and
 28

1 websites visited by a user in order to inform the user whether those applications or websites are
2 over-utilizing the mobile device's system resources or battery.

3 62. Moreover, as to data that Carrier IQ does transmit anonymously, because the
4 information stored in the HTTPS URLs captured by Carrier IQ contain identifying and sensitive
5 information such as passwords, names, addresses, and bank account numbers, their claims that
6 Carrier IQ is safe and does not violate consumer privacy are also inaccurate.

7 63. By virtue of Plaintiff's regular use of his Smartphone, Plaintiff's private and
8 personal communications have been illegally intercepted and transmitted by Carrier IQ as a
9 consequence of HTC's illegal installation of IQ Agent on his device.

10 **VIII. Plaintiff's Allegations**

11 64. Plaintiff Michael Allan purchased his HTC EVO 4G Smartphone from
12 Walmart.com on August 11, 2011. The HTC EVO 4G carries Google's Android operating
13 system.

14 65. Plaintiff activated service on his Smartphone with the cellular carrier Sprint.

15 66. Unbeknownst to Plaintiff, HTC altered the Google Android system by installing
16 IQ Agent on Plaintiff's HTC EVO 4G prior to Plaintiff's purchase.

17 67. Plaintiff learned of IQ Agent from the media on December 7, 2011 by reading
18 about the Carrier IQ phone tracking scandal on Google's News website.

19 68. Plaintiff then downloaded "Carrier IQ Detector" from the Android marketplace
20 onto his Smartphone. "Carrier IQ Detector" is one of the many apps that have proliferated in the
21 wake of the Carrier IQ scandal that allow users to detect whether their Android devices have IQ
22 Agent installed on them.

23 69. Between August and December, 2011, Plaintiff used his Smartphone in its
24 normal course, visiting websites, reading and sending e-mail, and downloading and using apps.
25 Plaintiff visited numerous websites secured by the HTTPS protocol.
26

CLASS ACTION ALLEGATIONS

I. Class Definition

70. Plaintiff brings this action under Rule 23(b)(3) of the Federal Rules of Civil Procedure, or, in the alternative, under Rule 23(b)(2), on behalf of himself and a proposed nationwide Class consisting of:

All persons or entities in the United States who own or have owned HTC brand mobile devices on which Carrier IQ's software was installed or embedded.

Excluded from the proposed Class are: Defendants; Defendants' affiliates and subsidiaries; any person, firm, trust, corporation, or other entity related to or affiliated with Defendants; and the judge or magistrate judge to whom this case is assigned, as well as those judges' immediate family members.

II. Numerosity

71. The Class is so numerous that the individual joinder of all members is impracticable. While the exact size of the Class and the identify of individual Class Members is unknown and cannot be ascertained without appropriate discovery, Plaintiff is informed and believes that the Class includes at least millions of individual consumers nationwide.

III. Commonality

72. Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary from Class Member to Class Member, and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to whether:

- i. Carrier IQ designed IQ Agent and/or other Carrier IQ tracking software, software that captures and transmits user data to cellular carriers;
- ii. HTC installed IQ Agent and/or other Carrier IQ tracking software on its Android mobile devices, including tablets and Smartphones;
- iii. IQ Agent and/or Carrier IQ tracking software captures user data including, but not limited to: when users turns their mobile devices on or off; which applications users download, open, and close; which applications crash on users' devices; where users'

1 devices are located; whether calls or text messages are received by users; which websites users
 2 visit; whether the websites users visit load properly; whether users' screens are on or off; which
 3 keys users press on the phone dialer, even if the phone numbers are not dialed; user devices'
 4 battery level, voltage, and temperature; and users' passwords and other private information
 5 entered into websites, including encrypted websites with the HTTPS prefix;

6 iv. IQ Agent and/or other Carrier IQ software intercepted the electronic
 7 communications of HTC Android device consumers within the meaning of the Federal Wiretap
 8 Act, 18 U.S.C. 2510, *et seq.*;

9 v. Carrier IQ violated the Federal Wiretap Act by designing and
 10 distributing IQ Agent and/or other tracking software and facilitating the interception and
 11 disclosure of electronic communications;

12 vi. HTC violated the Federal Wiretap Act by cooperating with Cellular
 13 Carriers and Carrier IQ in intercepting electronic communications by installing IQ Agent and/or
 14 other Carrier IQ software on its Android devices;

15 vii. HTC engaged in unfair, false, misleading, or deceptive acts or
 16 practices regarding the marketing and sale of Android devices in violation of California's Unfair
 17 Competition Law (UCL), CAL. BUS. & PROF.S CODE § 17200 *et seq.*;

18 viii. Class Members are entitled to statutory or other damages, civil
 19 penalties, punitive damages, restitution, and/or declaratory or injunctive relief.

20 **IV. Typicality**

21 73. Plaintiff's claims are typical of the Class Members' claims. Defendants'
 22 common course of conduct violated the Federal Wiretap Act and the California UCL in the same
 23 way and caused Class Members the same injuries. Likewise, Plaintiff and Class Members must
 24 prove the same facts in order to establish the same claims.

25 **V. Adequacy of Representation**

26 74. Plaintiff is an adequate Class Representative for the Class because he is a Class
 27 Member and his interests do not conflict with Class interests. Plaintiff retained counsel
 28 competent and experienced in consumer protection class actions, and together Plaintiff and

1 counsel intend to prosecute this action vigorously for the Classes' benefit. Plaintiff and his
2 counsel will fairly and adequately protect Class interests.

3 75. The Class can be properly maintained under Rule 23(b)(2). Defendants have acted
4 or refused to act, with respect to some or all issues presented in this Complaint, on grounds
5 generally applicable to the Class, thereby making appropriate final injunctive relief with respect
6 to the Class as a whole.

7 76. The Class can be properly maintained under Rule 23(b)(3). A class action is
8 superior to other available methods for the fair and efficient adjudication of this litigation because
9 individual litigation of each Class Member's claim is impracticable. Even if each Class Member
10 could afford individual litigation, the court system could not. It would be unduly burdensome if
11 millions of individual cases proceed. Likewise, individual litigation presents a potential for
12 inconsistent or contradictory judgments, the prospect of a race for the courthouse, as well as the
13 risk of an inequitable allocation of recovery among those with equally meritorious claims.
14 Individual litigation further increases the expense and delay to all parties and the courts because it
15 requires individual resolution of common legal and factual questions. By contrast, the class
16 action device presents far fewer management difficulties and provides the benefit of a single
17 adjudication, economies of scale, and comprehensive supervision by a single court.

18 **CLAIMS FOR RELIEF**

19 **FIRST CAUSE OF ACTION**

20 **(Violation of the Federal Wiretap Act, 18 U.S.C. § 2520)**

21 77. Plaintiff, individually and on behalf of the Class, incorporates by reference all of
22 the allegations contained in the preceding paragraphs of this Complaint.

23 78. Defendants Carrier IQ and HTC intentionally intercepted, endeavored to
24 intercept, or procured other persons to intercept or endeavor to intercept wire and/or electronic
25 communications as described herein, without the knowledge, consent, or authorization of
26 Plaintiff or the Class, in violation of 18 U.S.C. § 2511(1)(a).

27 79. Defendants Carrier IQ and HTC intentionally disclosed or endeavored to disclose
28 to another person the contents of wire and/or electronic communications, knowing or having

1 reason to know that the information was obtained through the interception of wire and/or
2 electronic communications in violation of 18 U.S.C. § 2511(c).

3 80. Defendants Carrier IQ and HTC intentionally used or endeavored to use the
4 contents of wire and/or electronic communications, knowing or having reason to know that the
5 information was obtained through the interception of wire and/or electronic communications in
6 violation of 18 U.S.C. § 2511(d).

7 81. As a result of these violations, Plaintiff and the Class suffered harm, including the
8 interception and transmission of sensitive user data.

9 82. As a result of these violations, Plaintiffs are entitled to appropriate relief,
10 including "such preliminary and other equitable or declaratory relief as may be appropriate;
11 statutory damages as set forth in 18 U.S.C. § 2520(c)(2); punitive damages in appropriate cases;
12 and a reasonable attorney's fee and other litigation costs reasonably incurred." *See* 18 U.S.C. §
13 2520(b), (c).

14 83. Plaintiff, for himself and the Class, seeks all such appropriate relief.

15 **SECOND CAUSE OF ACTION**
16 **(Violation of the California UCL, CAL. BUS. & PROF. CODE § 17200, *et seq.*)**

17 84. Plaintiff, individually and on behalf of the Class, incorporates by reference all of
18 the allegations contained in the preceding paragraphs of this Complaint.

19 85. Defendants' conduct alleged herein constitutes unfair and deceptive business acts
20 and practices in violation of CAL. BUS. & PROF. CODE § 17200, *et seq.*

21 86. Defendants' conduct is "unlawful" as it violates the Federal Wiretap Act, 18
22 U.S.C. § 2511.

23 87. Defendants' conduct is "unfair" because it offends Article 1 Section 1 of the
24 California Constitution and established public policy and/or is immoral, unethical, oppressive,
25 unscrupulous, and/or substantially injurious to customers.

26 88. Plaintiff and the Class in purchasing their smartphones surrendered more or
27 acquired less than they otherwise would have but for Defendants' conduct as alleged herein.
28

89. As a result of Defendants' conduct, Plaintiff and the Class have had the value of their smartphones diminished.

90. Plaintiff, on behalf of himself and the Class, seeks equitable relief to enjoin Defendants from the conduct constituting unfair competition as alleged herein and to restore to Plaintiff and the Class that which Defendants acquired by means of such unfair competition.

PRAYER FOR RELIEF

91. Plaintiff, on behalf of himself and the Class requests that the Court order the following relief and enter judgment against Defendants as follows:

i. An Order certifying the proposed Class and appointing Plaintiff and his counsel to represent the Class;

ii. An Order that Defendants be permanently enjoined from their improper activities and conduct described herein;

iii. An Order directing HTC to accept from Plaintiffs and Class Members returns of any HTC Android devices for full refund, with no restocking fee, for a period of six (6) months following the date of any such Order;

iv. A judgment awarding Plaintiff and the Class actual and compensatory damages in an amount according to proof;

v. A judgment awarding Plaintiff and the Class statutory damages in an amount computed in accordance with 18 U.S.C. § 2520(c);

vi. A judgment awarding Plaintiff and the Class restitution from Defendants in an amount according to proof, including without limitation, restitution of, disgorgement of, and/or the imposition of a constructive trust upon, all profits, benefits, and other compensation obtained by Defendants from their deceptive, misleading, and unlawful conduct alleged herein;

vii. A judgment awarding Plaintiffs and the Class punitive damages;

viii. Pre-judgment and post-judgment interest;

ix. Attorneys' fees and expenses and the costs of this action; and

1 x. All other and further relief as the Court deems necessary, just and
2 proper.

3 **JURY DEMAND**

4 Plaintiff hereby demands, on behalf of himself and the Class, a trial by jury.

5
6
7 Dated: December 22, 2011

By: 

8 Michael W. Sobol (State Bar No. 194857)

9 LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
10 275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
11 Telephone: (415) 956-1000
Facsimile: (415) 956-1008

12 *Attorneys for Plaintiff and the Proposed Class*
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28